UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

NXIVM CORP.,

Plaintiff,

-against- 1:14-cv-1375 (LEK/RFT)

TONI FOLEY, *et al.*,

Defendants.

**MEMORANDUM-DECISION and ORDER**

## I. INTRODUCTION

Plaintiff NXIVM Corporation ("Plaintiff") commenced this action on October 23, 2013 against Defendants Toni Foley ("Foley"), Joseph O'Hara ("O'Hara"), John Tighe ("Tighe"), Suzanna Andrews ("Andrews"), James Odato ("Odato"), and John Does 1 through 59 (collectively "Defendants"), asserting claims arising from Defendants' alleged unauthorized access of confidential and proprietary information contained on Plaintiff's password-protected website. Dkt. No. 1 ("Complaint"). The Complaint alleges violations of the Computer Fraud Abuse Act ("CFAA"), 18 U.S.C. § 1030, Stored Communications Act ("SCA"), 18 U.S.C. § 2071, as well as various state law causes of action arising from the same conduct on the part of Defendants. Presently before the Court are Motions to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) filed by Andrews, Odato, and O'Hara. Dkt. Nos. 27 ("Andrews Motion"); 31 ("Odato Motion"); 64 ("O'Hara Letter Request"). For the following reasons, the Motions to dismiss are granted. On September 10, 2015, Foley filed a Letter Motion requesting a conference. Dkt. No. 80 ("Foley Letter Motion"). Plaintiff filed a Letter Motion in response, requesting denial of Foley's Letter Motion. Dkt. No. 82 ("Plaintiff's Letter Motion"). Since Defendants' Motions to dismiss are

granted, the Court denies these Letter Motions as moot.

## II. BACKGROUND[1]

### A. Confidentiality Within the NXIVM System

Plaintiff is a for-profit corporation which sells professional success training programs, formerly known as Executive Success Programs. Compl. ¶ 1. Plaintiff provides its clients with training in areas such as internal ethics, logical analysis, and problem-solving skills. Id. ¶ 10. Plaintiff employs twelve field trainers to sell its products. Id. ¶ 22. Each field trainer maintains a client list, and collectively, the client lists are compiled and maintained by Plaintiff. Id. ¶¶ 23-24. These lists, taken together, comprise Plaintiff's entire client list. Id. ¶ 25. The client list includes every person who has enrolled in Plaintiff's course, and Plaintiff alleges that maintaining the confidentiality of client identities is of the utmost importance to Plaintiff's business model. Id. ¶ 27.

Plaintiff's program is based on the patent-pending system Rational Inquiry. Id. ¶ 10. Plaintiff maintains a license to use the Rational Inquiry system from the system's creator, First Principles. Id. ¶ 11. Under the terms of the license, Plaintiff is required to protect and maintain the confidentiality of the Rational Inquiry system. Id. In addition to the Rational Inquiry system, Plaintiff has developed its own proprietary written materials, methodologies, and educational philosophy, which are not available to the general public. Id. ¶¶ 13, 14, 16. Plaintiff charges "substantial fees" for its training services and programs, based on the company's confidential and

[1] Because this case is before the Court on a motion to dismiss for failure to state a claim, the allegations of the Complaint are accepted as true and form the basis of this section. See Boyd v. Nationwide Mut. Ins. Co., 208 F.3d 406, 408 (2d Cir. 2000); see also Matson v. Bd. of Educ., 631 F.3d 57, 72 (2d Cir. 2011) (noting that, in addressing a motion to dismiss, a court must view a plaintiff's factual allegations "in a light most favorable to the plaintiff and draw[] all reasonable inferences in her favor").

proprietary information and materials. Id. ¶ 15. Plaintiff requires anyone viewing its course material to sign a confidentiality agreement and anyone participating in an event sponsored by Plaintiff must sign a "long-form confidentiality agreement." Id. ¶¶ 17-18. Plaintiff alleges that no one is allowed to view any of its course materials or any information about its client lists without first agreeing to Plaintiff's confidentiality language. Id. ¶¶ 19, 31. Plaintiff does not actively advertise its courses, and instead relies primarily on word-of-mouth to generate prospective clients. Id. ¶ 21. A large portion of Plaintiff's revenue is derived from repeat clients, who continue to take additional seminars every year. Id. ¶ 29.

**B. Password-Protected Website**

Plaintiff maintains an interactive website for the exclusive use of its clients and staff. Id. ¶ 33. The website is password protected, meaning that it can only be accessed with a username and password, or by using a specialized formula. Id. ¶ 33. The level of access provided to a given user varies depending on the user's particular role within Plaintiff's organization. Id. ¶ 35. A user with the most basic level of access is not able to view confidential or proprietary information, such as Plaintiff's client or coaching lists. Id. ¶ 36. Conversely, a user who has taken a more active role, such as a "coach," is given a higher level of access, including access to confidential and proprietary information such as coach lists, client lists, the coach evaluation page, and business and promotional materials contained on the "Knowledge Base" page of Plaintiff's website. Id. ¶¶ 37-49.

**C. Suspicion of Unauthorized Access**

The Complaint states that "[i]n late 2011, suspicions arose as to whether unauthorized users were accessing the Password Protected Website." Id. ¶ 52. Plaintiff then conducted an investigation, and in early 2012 Plaintiff discovered that the login credentials of Client P, a former

coach who had not accessed the website since 2003, had been used to access the website "on hundreds of occasions between 2006 and 2011." Id. ¶¶ 53, 57. Client P confirmed that she had not given her credentials to anyone. Id. ¶ 55. The investigation also revealed that multiple users had used Client P's credentials from multiple internet protocol ("IP") addresses. Id. ¶ 58. Plaintiff alleges that Defendants shared and exchanged Client P's credentials amongst themselves and with others, in order to obtain proprietary information contained on the password-protected website, such as Plaintiff's client and coach lists. Id. ¶¶ 58-59. Plaintiff was able to match some of the IP addresses that used Client P's credentials with IP addresses known to be used by Defendants. Id. ¶ 61. The majority of IP addresses used to log in with Client P's credentials remain unidentified pending further discovery. Id.

**D. Defendant Foley**

Foley is Plaintiff's former client. Id. ¶ 2. Plaintiff alleges that on three separate occasions, Client P's credentials were used to access the protected portions of the website using IP addresses that Foley also used on those dates. Id. ¶ 62. Specifically, the Complaint alleges that Foley accessed the website on August 23, 2010, January 5, 2011, and March 15, 2011. Id. After reviewing the records from the website, Plaintiff's information technology ("IT") staff believes that Foley accessed Plaintiff's coach list, calendar of events, humanities events page, coach evaluation tool, and Vanguard Week (Plaintiff's private annual corporate retreat) information list. Id. ¶ 63. Plaintiff also believes that Foley accessed portions of the website that would allow her to improperly obtain the necessary information to create an unofficial client list. Id.

**E. Defendant O'Hara**

O'Hara is Plaintiff's former attorney. Id. ¶ 3. Plaintiff alleges that O'Hara misrepresented

that he was licensed to practice law in New York State. Id. Plaintiff alleges that O'Hara used Client P's credentials to access the website on February 3, 2010 and March 15, 2011. Id. ¶ 64. Plaintiff further alleges that on February 3, 2010, O'Hara and Foley communicated via telephone at least twenty times, both before and after O'Hara accessed the website. Id. Plaintiff believes that O'Hara accessed Plaintiff's calendar of events, humanities events page, and the Magnificence Reports, which would have allowed him to create an unofficial client list. Id. ¶ 66. Plaintiff also believes that O'Hara sent the client list to various members of the media and other third parties in an attempt to harass Plaintiff and its clients. Id. ¶ 90.

**F. Defendant Tighe**

Tighe is the author of a blog titled "Saratoga in Decline." Id. ¶ 4. Plaintiff alleges that an IP address attributed to Tighe used Client P's credentials to access the website on seventeen dates between July and November 2010. Id. ¶ 67. Plaintiff asserts that Tighe accessed Plaintiff's coach list, calendar of events, humanities events page, humanities questionnaire, goals reporting tool, testimonials page, and Vanguard Week information page. Id. ¶ 68. Tighe published the names and contact information from Plaintiff's confidential coach list on his blog on August 7, 2011, including the following statement:

> This list only includes the names and rank of current recruiters and coaches who actively prey and profit from the insecurities and weaknesses of their neighbors, business associates, friends and in the most extreme cases their own families including parents and even their own children. I have no mercy or sympathy for these people at all.

Id. ¶ 92. Plaintiff further alleges that Tighe used information obtained on the protected portions of the website to harass Plaintiff's clients. Id. ¶ 85. Specifically, the Complaint alleges that Tighe showed up at Vanguard Week in September 2010, approached a group of Plaintiff's clients' children,

and stated that "he picked up little children and ran away with them to protect them from a bad man." Id. ¶ 85. The Complaint also alleges that Tighe showed up at Vanguard Week in 2011, at a NXIVM executive's private birthday parties in July 2010 and 2011, and at Plaintiff's private corporate winter party in January 2011. Id. ¶ 86. The details of these events were only available on the password-protected portions of Plaintiff's website. Id. Tighe allegedly took photographs of Plaintiff's clients and published some of these photographs on his blog along with derogatory statements about Plaintiff and its clients. Id. The Complaint alleges that Tighe made a statement on his blog indicating that his only purpose for attending Plaintiff's events was to harass Plaintiff's clients and staff. Id. Police reports were filed regarding Tighe's harassment at these events. Id.

**G. Defendant Andrews**

Andrews is a professional freelance journalist who authored an article about Plaintiff that appeared in Vanity Fair magazine in October 2010. Id. ¶ 5; Andrews Mot at 1. Plaintiff alleges that an IP address attributed to Andrews used Client P's credentials to access the website on four separate dates between July and September 2010. Compl. ¶ 69. Plaintiff asserts that Andrews accessed Plaintiff's coach list, Magnificence Reports, and Vanguard Week information page. Id. ¶ 70.

**H. Defendant Odato**

Odato has authored numerous articles covering Plaintiff while employed by the Albany Times Union. Id. ¶ 6. Odato began writing about Plaintiff in September 2007, and in total has written at least thirty-five articles involving Plaintiff. Id. ¶¶ 71-72. Plaintiff alleges that Odato has been acquainted with O'Hara since at least February 2007, and the two have regularly communicated since that time via telephone and email. Id. ¶ 72. Plaintiff believes that Odato obtained Client P's credentials from O'Hara. Id. On one particular occasion, an hour after Odato and O'Hara spoke on

the phone, an IP address registered to Odato's employer, the Times Union, used Client P's credentials to access the website. Id. ¶ 74. Plaintiff alleges that Odato accessed the Goal Reporting Tools, humanities questionnaire, Vanguard Week, and Magnificence Reports page, which could have enabled him to create an unofficial list of Plaintiff's clients. Id. ¶¶ 75-76. Odato published a story on October 8, 2007, six days after allegedly accessing the protected portions of the website. Id. ¶ 77. In the story, Odato admitted to having a copy of Plaintiff's client list, and included the names of two of Plaintiff's clients in the article. Id. ¶¶ 77-78. Plaintiff asserts that the client list is proprietary, confidential, and not available to the general public. Id. ¶ 78.

**I. John Doe Defendants**

Plaintiff also names as Defendants several John Doe Defendants, identified only by their IP addresses, who Plaintiff alleges accessed Plaintiff's password-protected website without authorization between 2006 and 2011. Id. ¶ 7.

**J. Summary of the Complaint**

The Complaint alleges that O'Hara, Foley, Tighe, and others targeted individuals on the client list in order to harass them. Id. ¶ 87. The Complaint also alleges that O'Hara, Foley, Tighe, and others exchanged Plaintiff's confidential and proprietary client and coach lists with each other. Id. ¶ 88. Plaintiff alleges that these Defendants conspired with each other and others to harass Plaintiff's clients and to cause harm to Plaintiff. Id. ¶ 89.

Plaintiff alleges that Defendants violated the CFAA by intentionally and without authorization accessing protected portions of Plaintiff's website, database, and server, causing "damage" by compromising the integrity of the data contained therein and "loss" in excess of $5,000.00. Id. ¶¶ 93-103. Plaintiff also alleges violations of the SCA against all Defendants. Id.

¶¶ 104-111. The Complaint asserts the following state law claims against O'Hara, Foley, and Tighe: (1) misappropriation of trade secrets, id. ¶¶ 112-122; (2) conversion, id. ¶¶ 123-126; (3) tortious interference with a contractual relationship, id. ¶¶ 127-134; (4) tortious interference with prospective business relations, id. ¶¶ 135-137.

**K. Procedural History**

Plaintiff commenced this action on October 22, 2013 in the Western District of New York. Compl. The case was transferred to the Northern District on November 13, 2014. Dkt. No. 45 ("Transfer Order"). On September 30, 2014, Andrews filed a Motion to dismiss, arguing that any claims against her are time-barred. Andrews Mot. Plaintiff filed a Response, Dkt. No. 53 ("Response-Andrews"), and Andrews in turn filed a Reply, Dkt. No. 62 ("Andrews Reply"). On October 1, 2014, Odato filed a Motion to dismiss, arguing that the claims asserted against him are also time-barred. Odato Mot.[2] Plaintiff filed a Response, Dkt. No. 55 ("Response-Odato"), and Odato filed a Reply, Dkt. No. 60 ("Odato Reply").

On February 23, 2015, O'Hara filed a Letter Request seeking to have the claims against him dismissed, arguing that the claims against him are also time-barred. O'Hara Letter Request. O'Hara, a *pro se* Defendant, is currently incarcerated at the Metropolitan Detention Center in Brooklyn, New York. Id. In light of O'Hara's *pro se* status, the Court construed his Letter Request as a motion to dismiss pursuant to Rule 12(b)(6). See Dkt. No. 65 ("February Text Order"). Plaintiff filed a

[2] In considering a motion to dismiss under Rule 12(b)(6), the Court must "limit itself to a consideration of the facts that appear on the face of the complaint." Ryder Energy Distrib. Corp. v. Merrill Lynch Commodities Inc., 748 F.2d 774, 779 (2d Cir. 1984). Odato filed Affidavits and Exhibits with his Motion, which present additional evidence to the Court. See generally Dkt. Nos. 31-2 to 31-12. The Court may not consider these Affidavits and Exhibits for the purposes of deciding Odato's 12(b)(6) Motion. Ryder Energy Distrib. Corp., 784 F.2d at 779.

Response, Dkt. No. 67 ("Response-O'Hara"), and O'Hara filed a Reply, Dkt. No. 72 ("O'Hara Reply").

## III. LEGAL STANDARD

To survive a motion to dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure, a "complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 663 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)); see also FED. R. CIV. P. 12(b)(6). A court must accept as true the factual allegations contained in a complaint and draw all inferences in favor of a plaintiff. See Allaire Corp. v. Okumus, 433 F.3d 248, 249-50 (2d Cir. 2006). A complaint may be dismissed pursuant to Rule 12(b)(6) only where it appears that there are not "enough facts to state a claim to relief that is plausible on its face." Twombly, 550 U.S. at 570. Plausibility requires "enough fact[s] to raise a reasonable expectation that discovery will reveal evidence of [the alleged misconduct]." Id. at 556. The plausibility standard "asks for more than a sheer possibility that a defendant has acted unlawfully." Iqbal, 556 U.S. at 678 (citing Twombly, 550 U.S. at 556). "[T]he pleading standard Rule 8 announces does not require 'detailed factual allegations,' but it demands more than an unadorned, the-defendant-unlawfully-harmed-me accusation." Id. (citing Twombly, 550 U.S. at 555). Where a court is unable to infer more than the mere possibility of the alleged misconduct based on the pleaded facts, the pleader has not demonstrated that she is entitled to relief and the action is subject to dismissal. See id. at 678-79.

## IV. DISCUSSION

In the Motions to dismiss presently before the Court, Defendants argue that Plaintiff's CFAA and SCA claims are untimely. When a defendant raises a statutory bar such as the statute of

limitations as an affirmative defense, dismissal under Rule 12(b)(6) is appropriate if "it is clear from the face of the complaint, and matters of which the court may take judicial notice, that the plaintiff's claims are barred as a matter of law." Staehr v. Hartford Fin. Servs. Grp., 547 F.3d 406, 425 (2d Cir. 2008). Since the statute of limitations is an affirmative defense, the burden is on the defendant to show that a claim is untimely. Bano v. Union Carbide Corp., 361 F.3d 696, 710 (2d Cir. 2004). Defendants can generally satisfy this burden by demonstrating when the cause of action accrued. FTA Mkt. Inc. v. Vevi, Inc., No. 11 CV 4789, 2012 WL 383945, at *3 (S.D.N.Y. Feb 1, 2012). However, since the burden lies with the defendant, the plaintiff is not expected to anticipate potential affirmative defenses, or to affirmatively plead facts in avoidance of such defenses. Abbas v. Dixon, 480 F.3d 636, 640 (2d Cir. 2007). Thus, for a court to dismiss an action based on the statute of limitations at the 12(b)(6) stage, a plaintiff must effectively "plead[] itself out of court." In re marchFIRST Inc., 589 F.3d 901, 904-09 (7th Cir. 2009).

**A. Computer Fraud and Abuse Act**

The CFAA creates a private cause of action against a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." Penrose Comput. Marketgroup, Inc. v. Camin, 682 F. Supp. 2d 202, 207 (N.D.N.Y. 2010). The civil cause of action covers "[a]ny person who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g). An action under the CFAA must be brought "within two years of the date of the act complained of or the date of the discovery of the damage." Id. "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." Id. § 1030(e)(8). Stated differently, the statute of limitations begins to run either when the unlawful access takes place, or on the date the unlawful access is

discovered, whichever is later. FTA Mkt. Inc., 2012 WL 383945, at * 3.

**B. Stored Communications Act**

The SCA makes it a crime to "intentionally access[] without authorization a facility through which an electronic communication service is provided; or intentionally exceed[] an authorization to access that facility; and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a). The civil cause of action provision of the SCA provides that "any . . . person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind" may file suit. Id. § 2707(a). A civil action under the SCA must be commenced no "later than two years after the date upon which the claimant first discovered or had reasonable opportunity to discover the violation." Id. § 2707(f). "In other words, the limitations period begins to run when the plaintiff discovers that, or has information that would motivate a reasonable person to investigate whether, someone has intentionally accessed the facility through which an electronic communication service is provided" and thereby obtained unauthorized access to a stored communication. Sewell v. Bernardin, No. 14-3143, 2015 WL 4619519, at *3 (2d Cir. Aug. 4, 2015) (quoting 18 U.S.C. § 2701(a)).

**C. Sewell v. Bernardin**

The Second Circuit recently clarified how the statutes of limitation operate under the civil enforcement provisions of both the CFAA and SCA in Sewell. 2015 WL 4619519. In Sewell, the plaintiff alleged that the defendant violated the CFAA and SCA by gaining access to her email and Facebook accounts without her permission. Id. at *1. She discovered that her e-mail account may have been compromised on or about August 1, 2011, because her password had been altered. Id.

She discovered that her Facebook account may have been compromised on February 24, 2012, because her password had also been changed. Id. The district court granted the defendant's motion to dismiss with respect to all of the plaintiff's claims, finding that the claims were time-barred because the plaintiff became aware that the integrity of her computer had been compromised on August 1, 2011, but did not file suit until January 2, 2014. Id. at *3. The court reasoned that the plaintiff's reasonable opportunity to discover the full scope of defendant's alleged illegal activity began on August 1, 2011, more than two years before she filed her lawsuit. Id.

The Second Circuit agreed with the district court's finding regarding the plaintiff's e-mail account, but disagreed with the finding as to the plaintiff's Facebook account. Id. The court noted that under the SCA, the statute of limitations begins to run when the plaintiff first had a reasonable opportunity to discover that someone had intentionally accessed her account without authorization. Id.[3] Specifically, this opportunity arose "as soon as she discovered that she could not obtain access to that account because her password had been altered." Id. Thus, for the plaintiff's AOL account, the statute began to run when she first discovered that her information may have been compromised on August 1, 2011. Id. at *4. For her Facebook account, the statute began to run on February 24, 2012. Id. The court clarified that under the CFAA, "the statute of limitations began to run when the [plaintiff] learned that the integrity of her account had been impaired." Id. at *3. Since the plaintiff had no reason to suspect that her accounts had been compromised prior to discovering that her

[3] In Sewell, the Second Circuit only addressed the statute of limitations issue. The court specifically noted that whether the AOL and Facebook computers to which the defendant gained access were protected under the CFAA was not at issue on appeal, see Sewell, 2015 WL 4619519 at *4 n.6, nor did the court determine whether impairment to the integrity of the information contained in plaintiff's accounts was sufficient to constitute "damage" under the CFAA, see id. at *3-4. Having found that Plaintiff's CFAA claims and SCA claims are untimely, the Court finds it unnecessary to evaluate whether Plaintiff has alleged sufficient "damage" under these statutes.

passwords had been changed, the court's statute of limitations analysis was the same under both statutes. However, in some situations, as in the present case, the CFAA claim will accrue when a plaintiff first discovers that his or her account has been compromised, and the SCA claim accrues when the plaintiff first has a reasonable opportunity to discover that his or her account has been compromised. See generally id.

The court noted that the "statutes of limitations governing claims under the CFAA and SCA, as we understand them, may have troubling consequences in some situations. Even after a prospective plaintiff discovers that an account has been hacked, the investigation necessary to uncover the hacker's identity may be substantial." Id. at *5. The court noted that a plaintiff may be able to avoid a statute of limitations problem by initiating a lawsuit against John or Jane Doe defendants, so long as the plaintiff identifies the defendants within two years of discovery or after having a reasonable opportunity to discover damage to a protected computer. Id.

**D. Plaintiff's CFAA and SCA Claims are Untimely**

Recognizing that the statute of limitations is an affirmative defense, and that Defendants bear the burden of showing that the claims are untimely, the Court finds that Plaintiff's CFAA and SCA claims are untimely. As clarified in Sewell, the statute of limitations under the CFAA begins to run as soon as a plaintiff discovers that his or her computer has been impaired, and under the SCA, the statute begins to run as soon as a plaintiff has a reasonably opportunity to discover unauthorized access to his or her account.

In the present case, Plaintiff states that it first became suspicious that unauthorized users were accessing the password-protected portions of its website "in late 2011." Compl. ¶ 52. Plaintiff then conducted an investigation, and "after January 2012," was able to determine that some of the IP

addresses that wrongfully accessed the site belonged to Defendants. Resp.-Andrews at 3. Accordingly, the limitations period for the CFAA claim began to run when Plaintiff first became aware that its accounts may have been compromised in "late 2011," and the limitations period for the SCA claim began as soon as Plaintiff had a reasonable opportunity to discover unauthorized access to its network. See Sewell, 2015 WL 4619519, at *5. The statute of limitations is not tolled while Plaintiff conducted its internal investigation. Id.

Plaintiff commenced this action on October 23, 2013. Compl. Therefore, in order for its SCA claims to be timely, Plaintiff must not have had a reasonable opportunity to discover the alleged unauthorized access to its website prior to October 23, 2011, and in order for its CFAA claims to be timely, Plaintiff must not have discovered unauthorized access to the website prior to October 23, 2011. Although the Complaint is generally specific and detailed, including the dates on which each Defendant allegedly accessed the password-protected website, Plaintiff offers only the vague statement that it discovered the alleged unauthorized access "in late 2011." Compl. ¶ 52. Plaintiff offers no other facts explaining how or when it discovered the alleged damage "in late 2011," either in the Complaint or in any of its responses to Defendants' Motions. However, Plaintiff admits to having concerns about the statute of limitations when it commenced this action. See Dkt. No. 5-6 ("Wolford Affidavit") at ¶ 3. While Plaintiff is not required to anticipate affirmative defenses in its Complaint, see Bano, 361 F.3d at 710, Plaintiff does not provide additional facts or arguments to clarify when in 2011 it discovered unauthorized access to its website. Accordingly, the Court is limited in the inferences that can be drawn in Plaintiff's favor as to the timeliness of the CFAA and SCA claims. Conversely, the Complaint explains in great length the importance Plaintiff places in maintaining the confidentiality of its password-protected site, as well as Plaintiff's awareness that

various Defendants were in possession of confidential material that was only maintained on Plaintiff's website.

Plaintiff claims that it failed to launch an investigation prior to 2012 because the information published by Defendants "was legitimately accessible to [Plaintiff's] current coaches, field trainers and staff," and therefore, Plaintiff did not have reason to suspect that the confidential information on its website had been compromised. Resp.- Andrews at 19. However, Plaintiff's Complaint itself demonstrates that Plaintiff had knowledge that its website was being accessed by unauthorized individuals as early as October of 2007. See Odato Mem. at 15-16. For example, the Complaint alleges that Odato admitted in an article published in the Times Union in 2007 that he had obtained a copy of Plaintiff's confidential client list, which was available only to "a limited number of individuals." Compl. ¶ 41. The coach list published by Tighe in August 2011 was available only to Plaintiff's coaches. Id. ¶¶ 37, 39-40, 91-92. Moreover, the Complaint alleges that between 2010-2011, Tighe attended numerous private events hosted by Plaintiff, the details of which were available only on the private calendar section of Plaintiff's website. Id. ¶¶ 84-86. Plaintiff does not allege that it suspected that this information was obtained from any source other than the password-protected sections of Plaintiff's website.

Moreover, the Complaint states that Plaintiff's internal IT department was able to link unauthorized access to the website with Defendants' IP addresses. Id. ¶¶ 58, 61. Plaintiff offers no explanation as to why Plaintiff's IT personnel did not investigate unauthorized access to the website immediately after the publication of the Andrews, Odato, or Tighe articles, which allegedly contained proprietary and confidential information that was available only on Plaintiff's website. Accordingly, for the purposes of the SCA claims, the Court finds that Plaintiff had a reasonable

opportunity to discover the alleged unauthorized access prior to October 23, 2011.

Under the CFAA, however, the statute of limitations begins to run as soon as a plaintiff discovers that his or her computer has been impaired. See Sewell, 2015 WL 4619519, at *4. In Sewell, the Second Circuit squarely rejected Plaintiff's argument that the statute of limitations is tolled while the plaintiff conducts an investigation. Sewell, 2015 WL 4619519, at *5. Rather, a plaintiff is instructed to initiate a lawsuit "against a Jane or John Doe defendant, but she must still discover the hacker's identity within two years of discovery or a reasonable opportunity to discover the violation to avoid dismissal." Id.

In addition to the allegations in the Complaint discussed above, which suggest that Plaintiff had reason to be aware of unauthorized access prior to October 23, 2011, Odato requests that the Court take judicial notice of testimony of one of Plaintiff's executive board members and a former client that was taken on September 21, 2011, showing that Plaintiff was aware that the security of its password-protected website had been impaired more than two years prior to commencing this action. Odato Mem. at 17-19.

Courts routinely "take judicial notice of the fact that press coverage, prior lawsuits, or regulatory filings contained certain information, without regard to the truth of their contents" to determine whether such matters were sufficient to trigger inquiry notice. Staehr, 547 F.3d at 425; see also Global Network Commc'ns, Inc. v. City of New York, 458 F.3d 150, 157 (2d Cir. 2006) ("A court may take judicial notice of a document filed in another court not for the truth of the matters asserted in the other litigation but rather to establish the fact of such litigation and related filings."). In Staehr, judicial notice of media reports, state court complaints, and regulatory filings was appropriate to show that "certain things were said in the press, and that assertions were made in

lawsuits and regulatory filings, which is all that is required to trigger inquiry notice. None of those materials were offered for the truth of the matter asserted." Staehr, 547 F.3d at 425. Further, a court may take judicial notice of the records of other court proceedings without converting a motion to dismiss to one for summary judgment. See Kramer v. Time Warner, Inc., 937 F.2d 767, 774 (2d Cir. 1991) (taking judicial notice on Rule 12(b)(6) motion of SEC filings and noting that "it is highly impractical and inconsistent with Federal Rule of Evidence 201 to preclude a district court from considering such documents when faced with a motion to dismiss"); see also 5–Star Mgmt., Inc. v. Rogers, 940 F. Supp. 512, 518 (E.D.N.Y. 1996) (taking judicial notice of pleadings in other lawsuits attached to defendants' motion to dismiss); Munno v. Town of Orangetown, 391 F. Supp. 2d 263, 269 (S.D.N.Y. 2005) (taking judicial notice of affidavits and pleadings submitted by plaintiff's counsel in other litigation, as well as letters written by plaintiff's counsel in other litigation).

Here, Odato requests that the Court take judicial notice of the testimony of Susan Dones ("Dones"), Plaintiff's former client, and Clare Bronfman ("Bronfman"), one of Plaintiff's executive board members. See Odato Mem. at 17-19. The testimony was provided on September 21, 2011, during a bench trial in a bankruptcy case involving Dones. Odato Mem. at 17-19; Dkt. No. 31-11 (Transcript, In re Dones, No. 10-45608 (2011 W.D. Wash. Bankr.) ("Transcript"). In this proceeding, Plaintiff's counsel directly questioned Dones about whether she provided confidential information from Plaintiff's website to O'Hara. Tr. at 57:01-60:25. Plaintiff's counsel specifically asked how O'Hara could have obtained copies of Plaintiff's client list, and accused Dones of "provid[ing] intranet access to Mr. O'Hara and the confidential client list of NXIVM." Id. at 57:25-58:01. This line of questioning also reflects that Plaintiff had knowledge that the Defendants in the present action were working together and communicating via e-mail about publicizing Plaintiff's

client list and using the calendar obtained on the intranet to disrupt Vanguard Week. Id. at 58:08-11 ("You mean to say, Ms. Dones, in all these communications with Mr. O'Hara about disrupting NXIVM's Vanguard Week with a client list, nobody had any discussions about where the client list came from?").

In the same proceeding, Bronfman also testified that she was aware that Tighe had access to information from the password-protected portions of Plaintiff's website. Id. at 90:3-12; 91:11-25. Bronfman stated that Tighe obtained the client list from "somebody who had access" and admitted that the client list he published came from Plaintiff's intranet. Id. This testimony establishes that Bronfman, an executive board member, as well as Plaintiff's counsel, were aware of unauthorized access to its website by two of the Defendants in the present action on September 21, 2011, which is more than two years before the case was commenced on October 23, 2013. The Court is not concerned with the truth of the statements made in the bankruptcy proceeding. Rather, the Court only cares that these statements were made. Plaintiff's counsel's questions to Dones, as well as Bronfman's testimony, show that Plaintiff was aware of unauthorized access to its website more than two years before it commenced this action. This clarifies that Plaintiff's discovery of the "damage" to its system in "late 2011" occurred prior to October 23, 2011.

The cases Plaintiff cites in opposition to taking judicial notice of this prior testimony miss the mark. Plaintiff argues that it is inappropriate to take judicial notice of facts that contradict statements made by the plaintiff in the complaint. See Resp.-Odato at 8-9 (citing Global Network Commc'ns, Inc., 458 F.3d at 154; Int'l Star Class Yacht Racing Ass'n v. Tommy Hilfiger U.S.A., Inc., 146 F.3d 70 (2d Cir. 1998); Johnson v. Levy, 812 F. Supp.2d 167, 177 (E.D.N.Y. 2011)). Here, the Court does not take the statements from the bankruptcy transcript for the truth of the matter

asserted, but limits their use to the issue of whether Plaintiff had notice of a potential breach prior to October 23, 2011. Moreover, the Court has not accepted the statements contained in the bankruptcy proceeding over those contained in the Complaint, but has instead used this testimony to clarify Plaintiff's vague statement that it first discovered unauthorized access in "late 2011."

Additionally, Plaintiff argues that since the website was not the only source of the information that Defendants allegedly accessed, the publication of confidential information alone was not sufficient to give Plaintiff notice that the integrity of its website had been impaired. Response-Odato at 20-21. In support of this argument, Plaintiff relies on Clark Street Wine & Spirits v. Emporos Systems Corp., 754 F. Supp. 2d 474, 486 (E.D.N.Y. 2010). In Clark Street Wine, the court denied the defendant's motion to dismiss the plaintiff's CFAA claim as untimely where the plaintiff received a letter informing it that its store had been a source of significant fraud activity more than two years prior to filing suit. Id. The court found that since the letter did not specifically indicate that the plaintiff's computer system had been compromised, plaintiffs were not necessarily aware of any impairment to their computer system. Id. While Plaintiff is correct that there must be some affirmative link between suspicions of fraudulent activity and a plaintiff's computer system in order for the statute of limitations to commence in a CFAA claim, the Court finds a critical distinction between Clark Street Wine and the present case. Here, the Complaint itself emphasizes that Defendants possessed information that was only available on Plaintiff's website, and that Plaintiff was aware that Defendants possessed this information more than two years before commencing this action. While it is true that Defendants could have acquired this information from a NXIVM client who misappropriated the information, the transcript from In re Dones shows that Plaintiff was aware that Defendants had obtained access to their website more than two years before

they commenced this action. Accordingly, Plaintiff's CFAA claims against Andrews, Odato, and O'Hara are subject to dismissal on the grounds that they were not filed within the applicable two-year statute of limitations.

**E. CFAA and SCA Claims Against Foley and Tighe**

A district court has the power to dismiss a complaint *sua sponte* for failure to state a claim upon which relief may be granted, as long as the procedure employed is fair and the plaintiff has an opportunity to be heard. Thomas v. Scully, 943 F.2d 259, 260 (2d Cir. 1991). Here, although Foley and Tighe have not filed their own motions to dismiss, the Court finds that dismissal of Plaintiff's CFAA and SCA claims against these Defendants is appropriate. Plaintiff has had the opportunity to file three responsive briefs on the issue of whether these claims are timely filed, and the Court finds that Plaintiff's CFAA and SCA claims against Foley and Tighe suffer from the same untimeliness issues as Plaintiff's claims against Andrews, O'Hara, and Odato. Consequently, Plaintiff's CFAA and SCA claims against Foley and Tighe are dismissed.

**F. State Law Claims**

Having dismissed Plaintiff's CFAA and SCA claims, the Court no longer has subject-matter jurisdiction over Plaintiff's remaining claims for misappropriation of trade secrets, conversion, tortious interference with a contractual relationship, and tortious interference with prospective business relations. A federal district court has supplemental jurisdiction over all state-law claims "that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy." 28 U.S.C. § 1367(a). A district court may decline to exercise supplemental jurisdiction where it "has dismissed all claims over which it has original jurisdiction." Id. § 1367(c). "[I]n the usual case in which all federal-law claims are eliminated before trial, the

balance of factors to be considered under the pendent jurisdiction doctrine—judicial economy, convenience, fairness, and comity—will point toward declining to exercise jurisdiction over the remaining state-law claims." Carnegie-Mellon Univ. v. Cohill, 484 U.S. 343, 350 n.7 (1988). Because Plaintiff's federal claims have been dismissed at this early stage of litigation, the Court declines to exercise supplemental jurisdiction over Plaintiff's state law claims.

## V. CONCLUSION

Accordingly, it is hereby:

**ORDERED**, that Defendant Suzanna Andrews' Motion (Dkt. No. 27) to dismiss is **GRANTED**; and it is further

**ORDERED**, that Defendant James Odato's Motion (Dkt. No. 31) to dismiss is **GRANTED**; and it is further

**ORDERED**, that Defendant Joseph O'Hara's Motion (Dkt. No. 64) to dismiss is **GRANTED**; and it is further

**ORDERED**, that Plaintiff's CFAA and SCA claims against Defendant Foley and Defendant Tighe are **DISMISSED**; and it is further

**ORDERED**, that Defendant Tony Foley's Letter Motion (Dkt. No. 80) for a conference is **DENIED** as moot; and it is further

**ORDERED**, that Plaintiff's Letter Motion (Dkt. No. 82) opposing a conference is **DENIED** as moot; and it is further

**ORDERED**, that Plaintiff's state law claims for the misappropriation of trade secrets, conversion, tortious interference with a contractual relationship, and tortious interference with prospective business relations are **DISMISSED without prejudice** pursuant to 28 U.S.C.

§ 1367(c)(3); and it is further

**ORDERED**, that Plaintiff's Complaint (Dkt. No. 1) is **DISMISSED**; and it is further

**ORDERED**, that the Clerk of the Court serve a copy of this Memorandum-Decision and Order on all parties in accordance with the Local Rules.

**IT IS SO ORDERED.**

DATED: September 17, 2015
Albany, New York

Lawrence E. Kahn
U.S. District Judge